

S T O R M ⚡ W ⚡ T C H

Dateline: 2023-11-28



GREYNOISE
LABS

S T O R M ⚡ W A T C H



Storm ⚡ Watch by GreyNoise Intelligence

GreyNoise Intelligence

TECHNOLOGY · UPDATED WEEKLY

GreyNoise Storm ⚡ Watch is a weekly podcast and livestream hosted by GreyNoise Intelligence (<https://www.greynoise.io>), a cybersecurity company that focuses on understanding internet noise. The show features hosts b MORE

<https://pod.greynoise-storm.watch/>















<https://show.greynoise-storm.watch/>



TAGSMAS
IS
COMING...



Tagvent Calendar 2023

01 	02	03	04 	05 	06 
07 	08 	09 	10 	11 	12 
13 	14 	15 	16 	17 	18 
19 	20 	21 	22 	23	24 

It's all good



<https://www.reuters.com/technology/us-britain-other-countries-ink-agreement-make-ai-secure-by-design-2023-11-27/>

US, Britain, other countries ink agreement to make AI 'secure by design'

By Raphael Satter and Diane Bartz

November 27, 2023 9:57 PM EST · Updated 7 hours ago



[1/2] Artificial Intelligence words are seen in this illustration taken March 31, 2023. REUTERS/Dado

Ruvic/Illustration/File Photo [Acquire Licensing Rights](#)



WASHINGTON, Nov 27 (Reuters) - The United States, Britain and more than a dozen other countries on Sunday unveiled what a senior U.S. official described as the first detailed international agreement on how

Newsletter | Daily.

Technology Roundup

From startups to the FAANGs, get the latest news and trends in the global technology industry.

Sign up





The United States, Britain, and 18 other countries have signed an agreement to make AI systems "secure by design." This is the first detailed international agreement on keeping AI safe from misuse. The agreement is non-binding and includes recommendations such as monitoring AI systems for abuse and protecting data from tampering. The director of the U.S. Cybersecurity and Infrastructure Security Agency, Jen Easterly, says this is an important step in prioritizing security in AI development. The rise of AI has raised concerns about its potential for harm, including disrupting democracy and causing job loss. Europe is ahead of the U.S. in regulating AI, with lawmakers drafting rules. The Biden administration has also been pushing for AI regulation. The agreement does not address the appropriate uses of AI or how data is gathered.



<https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war>

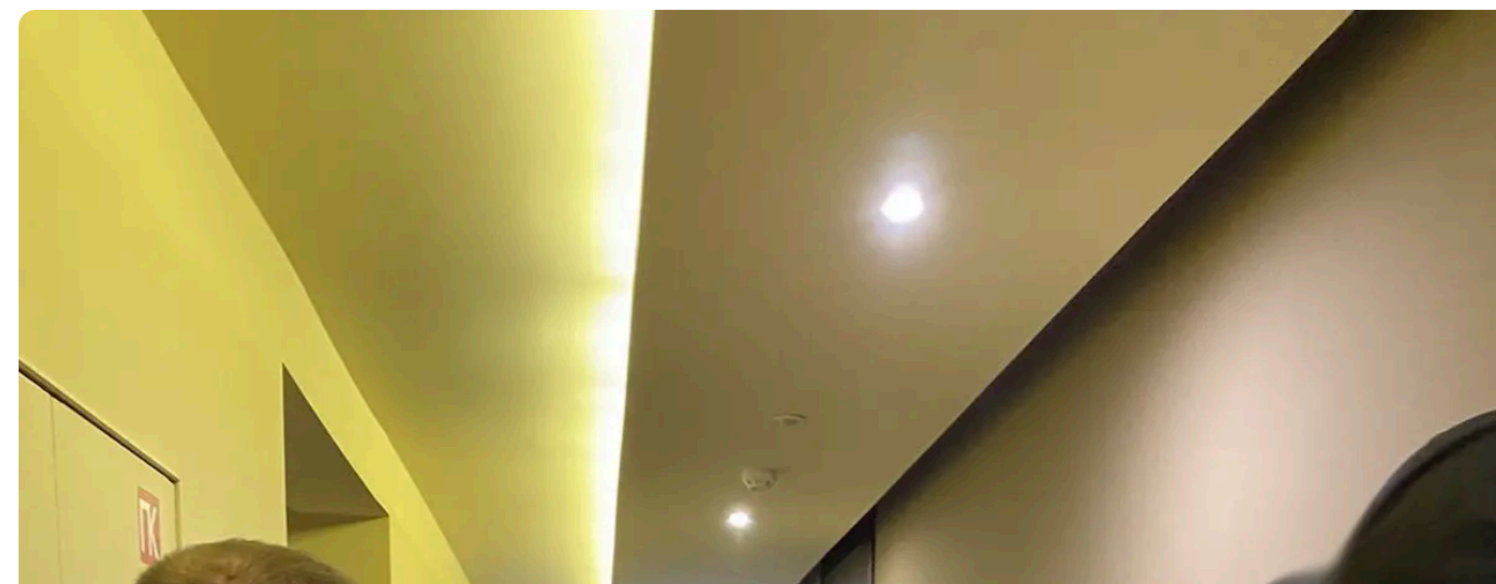
International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war

The ransomware gang is behind high-profile attacks that created losses of hundreds of millions of euros

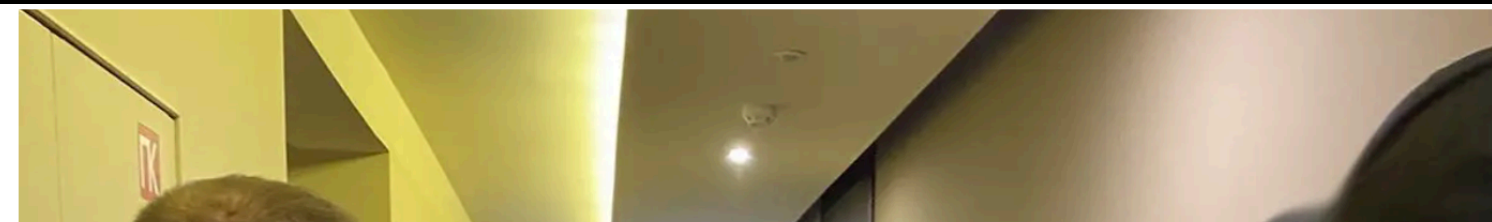
Part of the EU Policy Cycle - Empact

28
NOV
2023

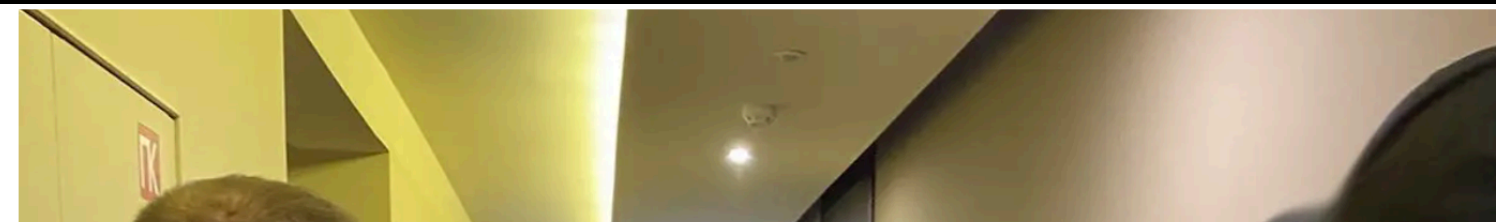
In an unprecedented effort, law enforcement and judicial authorities from seven countries have joined forces with Europol and Eurojust to dismantle and apprehend in Ukraine key figures behind significant ransomware operations wreaking havoc across the world. The operation comes at a critical time, as the country grapples with the challenges of Russia's military aggression against its territory.



In a significant international collaboration, law enforcement and judicial authorities from seven countries, along with Europol and Eurojust, have dismantled a major ransomware operation in Ukraine, arresting key figures behind the operation. Amidst the ongoing war and Russia's military aggression, 30 properties were searched in various regions of Ukraine on November 21, leading to the arrest of the 32-year-old ringleader and four of his most active accomplices. The operation was supported by over 20 investigators from Norway, France, Germany, and the United States, who were deployed to Kyiv to assist the Ukrainian National Police, while a virtual command post was activated at Europol's headquarters in the Netherlands to analyze the data seized during the house searches.



The individuals under investigation are believed to be part of a network responsible for high-profile ransomware attacks against organizations in 71 countries, causing losses of hundreds of millions of euros. The suspects had different roles within the organization, with some involved in compromising the IT networks of their targets, and others suspected of laundering cryptocurrency payments made by victims. The attackers used various techniques, including brute force attacks, SQL injections, and phishing emails, to break into networks and remain undetected, compromising as many systems as possible before triggering ransomware attacks. The investigation determined that the perpetrators encrypted over 250 servers belonging to large corporations.





BREAKING NEWS

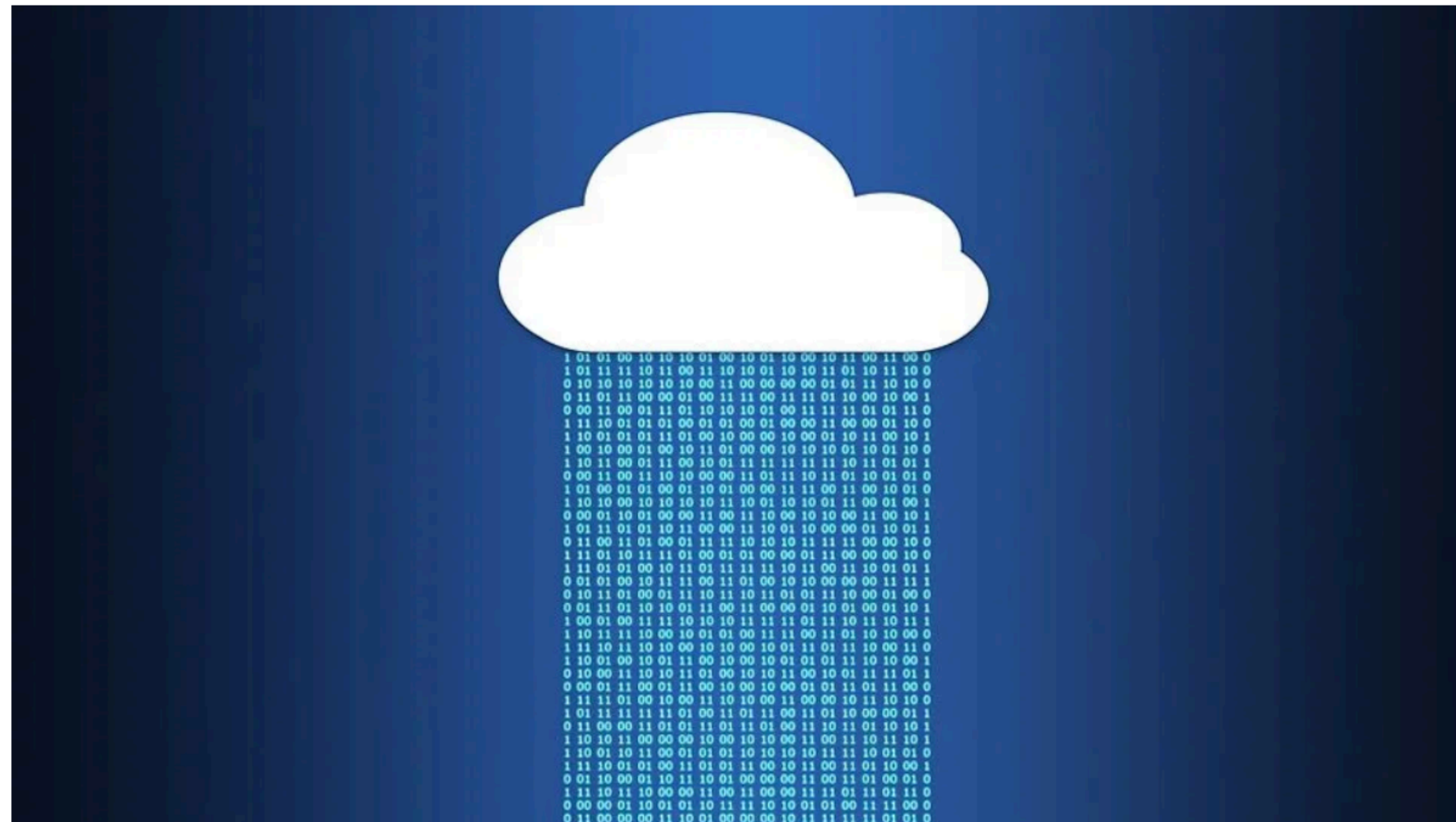
https://www.techradar.com/pro/security/top-file-sharing-service-hit-with-embarrassing-security-bug-that-reveals-admin-passwords

Pro > Security

Top file-sharing service hit with embarrassing security bug that reveals admin passwords

News By Sead Fadilpašić published about 23 hours ago

Three critical vulnerabilities were found in ownCloud



(Image credit: Pixabay)

Top file sharing service ownCloud has released three fixes to critical

MOST POPULAR MOST SHARED



1 Google Drive just made its best Android feature even better

2 Seagate has launched a massive 29TB hard disk drive that almost nobody noticed — but you can only buy the biggest ever HDD in a 2500TB storage device

3 China in a bull shop: One of the largest Chinese tech companies has announced a 'game-changing' 3,072-core RISC-V server that used an indigeneous CPU — on US soil

4 HP's lightest laptop makes the Dell XPS 13 look expensive and underpowered — The \$550 Pavilion Aero is the best value for money choice if you're looking for a superlight



ownCloud, a popular file-sharing service, has released three critical fixes for vulnerabilities that allowed hackers to steal admin credentials, modify and delete files, and redirect callbacks. These flaws were found in different components of the software and were given high severity scores. The first flaw, with a severity score of 10, can be used to steal login data and configuration information. The second flaw, with a severity score of 9.8, allows hackers to bypass authentication and access files. The third flaw, with a severity score of 9, is a subdomain validation bypass that can be used to redirect callbacks to a domain controlled by the attacker. These vulnerabilities can lead to data theft, identity theft, and phishing attacks. It is advised for users to apply the fixes immediately to ensure the security and integrity of the ownCloud platform. Other file-sharing services have also recently been breached, highlighting the importance of addressing these security issues.

VULNERABILITIES

CVE-2023-49103: ownCloud Critical Vulnerability Quickly Exploited in the Wild

Glenn Thorpe | November 27, 2023



ACTIVELY EXPLOITED

NEW

VULN



ownCloud
CVE-2023-49103



<https://www.greynoise.io/blog/cve-2023-49103-owncloud-critical-vulnerability-quickly-exploited-in-the-wild>

• 3 DAYS

10 DAYS

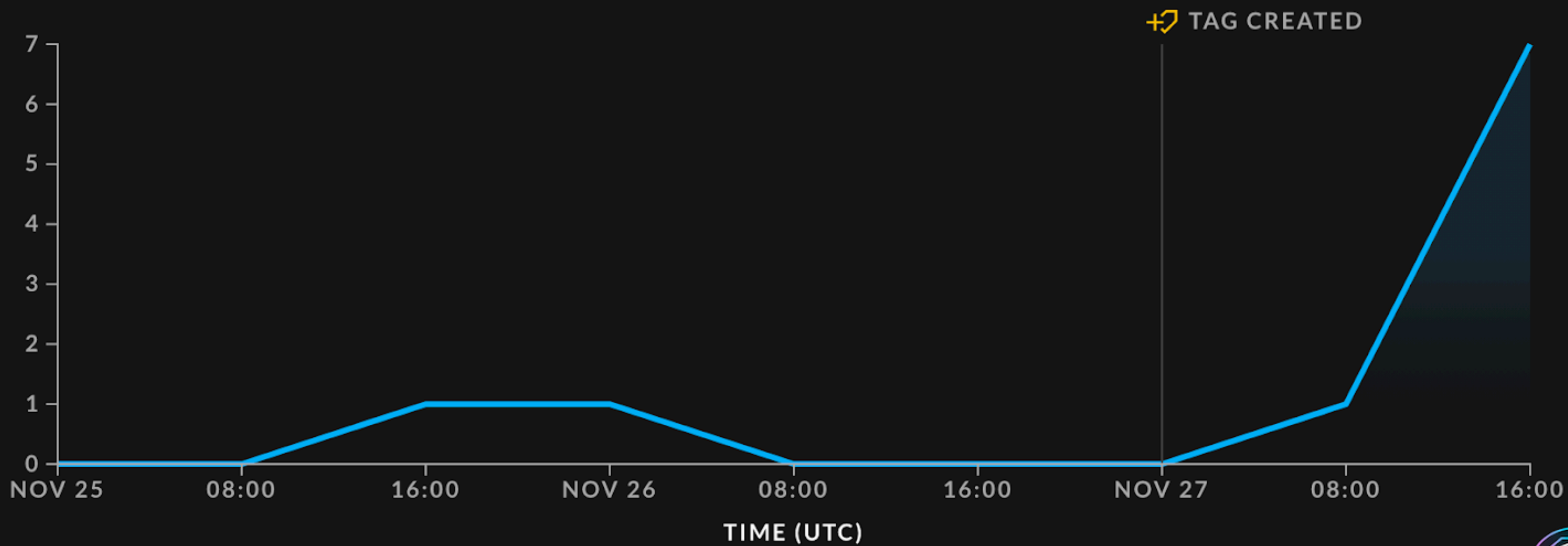
30 DAYS

November 24, 2023 - November 27, 2023

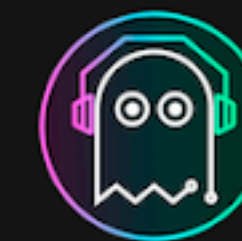
7

<https://viz.greynoise.io/tag/owncloud-graph-api-information-disclosure?days=3>

UNIQUE IPS OBSERVED BY GREYNOISE



owncloud-graph-api-information-disclosure



<https://www.akamai.com/blog/security-research/new-rce-botnet-spreads-mirai-via-zero-days>

InfectedSlurs Botnet Spreads Mirai via Zero-Days



Akamai SIRT
November 21, 2023

Share



Editorial and additional commentary by Tricia Howard

CONTENT WARNING: The threat actors responsible for this malware use racial slurs and other offensive content as filenames that appear in our screenshots. We did not redact them



The Akamai Security Intelligence Response Team (SIRT) has discovered two zero-day vulnerabilities with remote code execution (RCE) functionality exploited in the wild. The vulnerabilities are being actively exploited to build a distributed denial-of-service (DDoS) botnet. The botnet leverages the Mirai malware family and targets routers and network video recorder (NVR) devices with default admin credentials, installing Mirai variants when successful. The vulnerabilities have been reported to the vendors, and updates about impacted models and patch availability are expected in December 2023. The botnet activity primarily uses the older JenX Mirai malware variant and the hailBot Mirai variant. The C2 domains in this cluster contain racial epithets, offensive language, or generally inappropriate terms. The Akamai SIRT is working with CISA/US-CERT, and JPCERT to notify vendors of the impacted devices and has provided Snort and YARA rules to help defenders identify exploit attempts and possible infections in their environments. The SIRT plans to publish a follow-up blog post with additional details and deeper coverage of the devices and exploit payloads once the vendors and CERTs feel confident that responsible disclosure, patching, and remediation have run their course.

other offensive content as filenames that appear in our screenshots. We did not redact them



**NOW BACK TO OUR
REGULARLY SCHEDULED
PROGRAMMING**



Join TechCrunch+

Login

Search Q

TechCrunch+

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup Battlefield

More

Security

Ransomware 'catastrophe' at Fidelity National Financial causes panic with homeowners and buyers

Lorenzo Franceschi-Bicchierai @lorenzofb / 1:01 PM EST • November 27, 2023

Comment



TechCrunch Early Stage	April 25, 2024 Boston, MA
Tix On Sale For \$99	

<https://techcrunch.com/2023/11/27/ransomware-catastrophe-at-fidelity-national-financial-causes-panic-with-homeowners-and-buyers/>

Last Tuesday, Fidelity National Financial, or FNF, a real estate services company that [bills itself](#) as the “leading provider of title insurance and escrow services, and North America’s largest title insurance company,” [announced that it had experienced a cyberattack](#).





Join TechCrunch+

Login

Search

TechCrunch

Startup

Venture

Security

AI

Crypto

Apps

Events

Startup

More

Security

Ransomware 'catastrophe' at Fidelity National Financial causes panic with homeowners and buyers



TechCrunch
Early Stage

April 25, 2024

Boston, MA

Tix On Sale For \$99

Fidelity National Financial (FNF), a leading provider of title insurance and escrow services, recently experienced a significant cyberattack that has caused widespread concern and disruption. The attack was first announced in a regulatory filing with the U.S. Securities and Exchange Commission (SEC) on November 19, 2023. The company blocked access to certain systems as a containment measure, which resulted in disruptions to its business, affecting services related to title insurance, escrow, mortgage transactions, and technology to the real estate and mortgage industries.

 Image Credits: Lori Moffett/Bloomberg via Getty Images / Getty Images

Last Tuesday, Fidelity National Financial, or FNF, a real estate services company that [bills itself](#) as the “leading provider of title insurance and escrow services, and North America’s largest title insurance company,” [announced that it had experienced a cyberattack](#).





Join TechCrunch+

Login

Search

TechCrunch

Startup

Venture

Security

AI

Crypto

Apps

Events

Startup

More

Security

Ransomware 'catastrophe' at Fidelity National Financial causes panic with homeowners and buyers



TechCrunch
Early Stage

April 25, 2024

Boston, MA

Tix On Sale For \$99

The investigation into the incident revealed that an unauthorized third party gained access to certain FNF systems and stole certain credentials. The company has not yet disclosed the specific nature of the stolen credentials or the extent of the data breach.

The cyberattack has had significant downstream effects on the real estate industry, with many scheduled home-sale closings being halted as a result. The company's website was down at the time of reporting, and customers have reported difficulties in contacting FNF and its subsidiaries.

 Image Credits: Lori Moffett/Bloomberg via Getty Images / Getty Images

Last Tuesday, Fidelity National Financial, or FNF, a real estate services company that [bills itself](#) as the “leading provider of title insurance and escrow services, and North America’s largest title insurance company,” [announced that it had experienced a cyberattack](#).





Join TechCrunch+

Login

Search Q

TechCrunch+

Startups

Venture

Security

AI

Crypto

Apps

Events

Startup

More

Security

Ransomware 'catastrophe' at Fidelity National Financial causes panic with homeowners and buyers

Lorenzo Franceschi-Bicchierai @lorenzofb / 1:01 PM EST • November 27, 2023

Comment




TechCrunch
Early Stage

April 25, 2024

Boston, MA

Tix On Sale For \$99

 In August, a massive cyberattack targeted Rapattoni Corporation, a major provider of Multiple Listing Services (MLS) to regional real estate groups across the U.S. The attack rendered MLS systems unusable, preventing real estate markets from listing new homes, changing prices, marking homes as pending/contingent/sold, or listing open houses

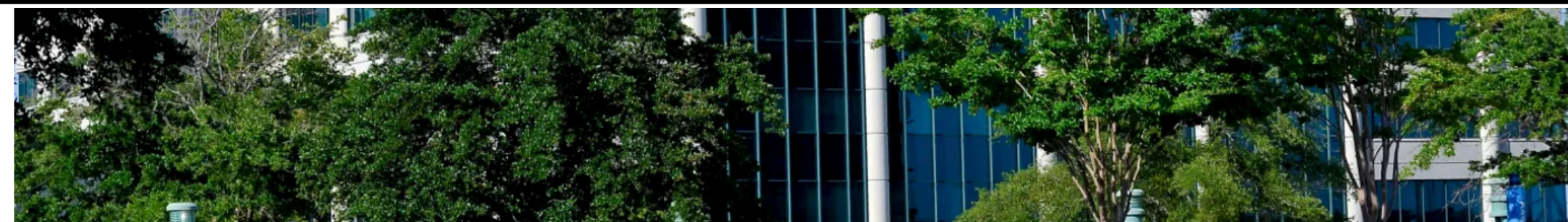


 Image Credits: Lori Moffett/Bloomberg via Getty Images / Getty Images

Last Tuesday, Fidelity National Financial, or FNF, a real estate services company that [bills itself](#) as the “leading provider of title insurance and escrow services, and North America’s largest title insurance company,” [announced that it had experienced a cyberattack](#).



United States
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 8-K
Current Report

Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934
Date of Report (date of earliest event reported): November 19, 2023

Fidelity National Financial, Inc.

(Exact name of Registrant as Specified in its Charter)

001-32630

(Commission File Number)

Delaware

16-1725106

(State or Other Jurisdiction of
Incorporation or Organization)

(IRS Employer Identification Number)

601 Riverside Avenue
Jacksonville, Florida 32204

(Addresses of Principal Executive Offices)

(904) 854-8100

(Registrant's Telephone Number, Including Area Code)

(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligation of the registrant under any of the following provisions:

- Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)
- Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)
- Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))
- Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Securities registered pursuant to Section 12(b) of the Act:

<u>Title of Each Class</u>	<u>Trading Symbol</u>	<u>Name of Each Exchange on Which Registered</u>
FNF Common Stock, \$0.0001 par value	FNF	New York Stock Exchange

Indicate by check mark whether the registrant is an emerging growth company as defined in Rule 405 of the Securities Act of 1933 (§230.405 of this chapter) or Rule 12b-2 of the Securities Exchange Act of 1934 (§240.12b-2 of this chapter).

Emerging growth company

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act.

<https://www.investor.fnf.com/static-files/c76988f7-929f-4fdb-99dc-2048586391e7>

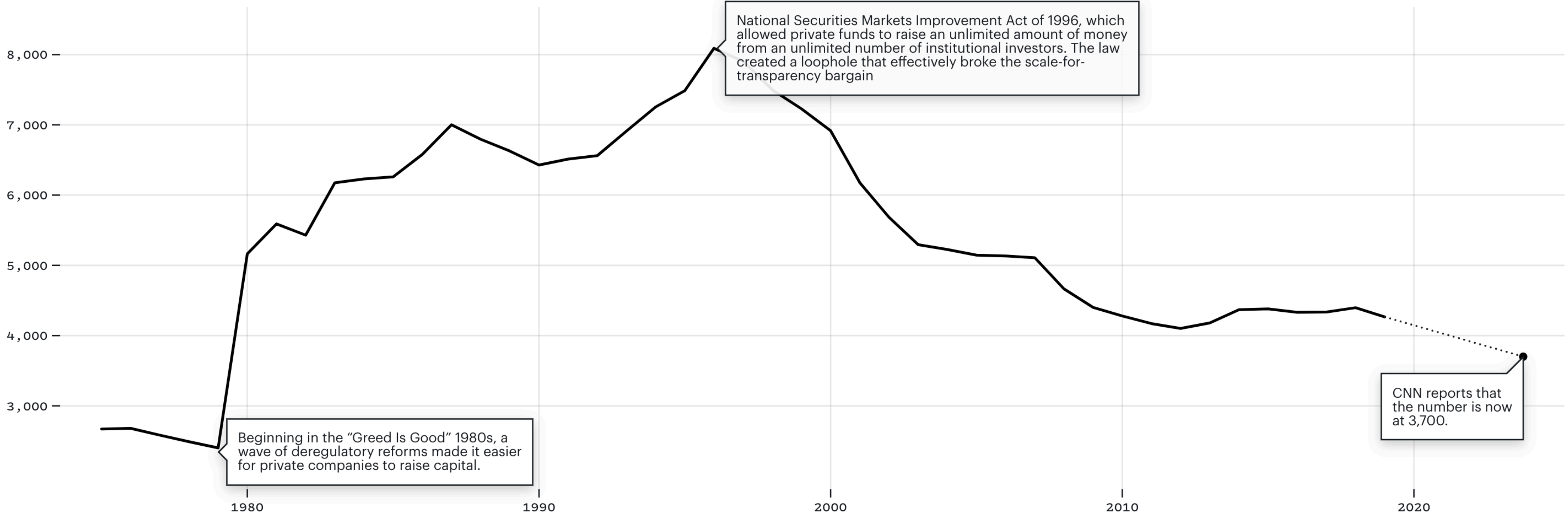
Fidelity National Financial, Inc. (“FNF” or the “Company”) recently became aware of a cybersecurity incident that impacted certain FNF systems, and promptly commenced an investigation, retained leading experts to assist the Company, notified law enforcement authorities, and implemented certain measures to assess and contain the incident. Among other containment measures, we blocked access to certain of our systems, which resulted in disruptions to our business. For example, the services we provide related to title insurance, escrow and other title-related services, mortgage transaction services, and technology to the real estate and mortgage industries, have been affected by these measures. Our majority-owned subsidiary,

F&G Annuities & Life, a leading provider of insurance solutions, was not impacted by the incident.

Based on our investigation to date, FNF has determined that an unauthorized

The Number Of Publicly Listed Companies Is In Decline Since It's Peak In 1996

↑ Count



Beginning in the "Greed Is Good" 1980s, a wave of deregulatory reforms made it easier for private companies to raise capital.

National Securities Markets Improvement Act of 1996, which allowed private funds to raise an unlimited amount of money from an unlimited number of institutional investors. The law created a loophole that effectively broke the scale-for-transparency bargain

CNN reports that the number is now at 3,700.

Data/info sources: [FRED](#); [CNN](#); [The Atlantic](#)

Auto parts giant AutoZone warns of MOVEit data breach

By **Bill Toulas**

November 21, 2023 01:03 PM 0



AutoZone is warning tens of thousands of its customers that it suffered a data breach as part of the Clop MOVEit file transfer attacks.

AutoZone is the leading retailer and distributor of automotive spare parts and accessories in the U.S., operating 7,140 shops in the country and also in Brazil, Mexico, and Puerto Rico.

The company has an annual revenue of nearly \$17.5 billion, employs 119,000 people, and its online shop is visited by 35 million users per month, according to similarweb.com stats.

Earlier this year, the Clop ransomware gang [exploited a zero-day MoveIT vulnerability](#) to breach

POPULAR STORIES



Google Drive users angry over losing months of stored data



New Rust-based SysJoker backdoor linked to Hamas hackers



Auto parts giant AutoZone warns of MOVEit data breach

POPULAR STORIES

By B



Auto
MOV
Auto
oper

AutoZone, a major auto parts retailer, has warned its customers of a data breach that occurred as part of the Clop MOVEit file transfer attacks. The breach, which was caused by a zero-day vulnerability, resulted in the compromise of data belonging to 184,995 people. The company took three months to determine the extent of the breach and what data was stolen. The leaked data, which was published by the Clop ransomware gang, does not include any customer information but does contain sensitive employee data. The gang is expected to receive over \$75 million in extortion payments from companies impacted by the MOVEit attacks. AutoZone has covered the cost of identity theft protection for affected individuals and advises them to remain vigilant for the next 24 months.

ing

or

The company has an annual revenue of nearly \$17.5 billion, employs 119,000 people, and its online shop is visited by 35 million users per month, according to similarweb.com stats.

Earlier this year, the Clop ransomware gang [exploited a zero-day MoveIT vulnerability](#) to breach



MOVEit Cyber Attack - Affected organizations (as of November 23, 2023)

By country <https://konbriefing.com/en-topics/cyber-attacks-moveit-victim-list.html>



CSO

Microsoft's bug bounty turns 10. Are these kinds of rewards making code more secure?

8 

Katie Moussouris, who pioneered Redmond's program, says folks are focusing on the wrong thing

https://www.theregister.com/2023/11/22/microsofts_bug_bounty_moussouris/



INTERVIEW Microsoft's bug bounty program celebrated its tenth birthday this year, and has paid out \$63 million to security researchers in that first decade – with \$60 million awarded to bug hunters in the past five years alone, according to Redmond.

While these days, the vulnerability disclosure and reward program seems like a no-brainer for a huge software concern, ten years ago "the bug bounty initiative was not free from internal resistance," recalled Aanchal Gupta, Microsoft corporate VP and deputy CISO.



From chaos to cadence: Celebrating two decades of Microsoft's Patch Tuesday

READ MORE →

In a [write-up](#) this week commemorating the program's first decade, Gupta recounts how it started with reports of vulnerabilities in a preview of Internet Explorer 11 and exploitation of holes in Windows 8.1. Back in 2013, the reward for flaws found in IE in preview was especially novel, she added.

"Although not pioneers in offering monetary incentives for external parties to report software security vulnerabilities, we were among the first to incentivize the discovery of issues in beta or preview products," Gupta wrote. "Our belief was that early identification and resolution of bugs, preferably before the product's general release, is paramount in customer protection."

Gupta also highlighted the bug bounty initiative's explosive growth, especially since 2018. In fiscal year 2019, for example, Microsoft "more than doubled the number of bounty reports, program participants, and awards compared to the previous year," she wrote. A year later, it awarded more than \$13 million to more than 300 security researchers across 15 categories, and also awarded larger prizes for more serious issues.

Microsoft's bug bounty program, which rewards security researchers for identifying software vulnerabilities, celebrated its 10th anniversary this year. Over the past decade, the program has paid out \$63 million, with \$60 million awarded in the last five years alone. The initiative faced internal resistance when it was first launched, but has since grown significantly, especially since 2018. In 2019, Microsoft doubled the number of bounty reports, program participants, and awards compared to the previous year. In 2020, the company introduced higher awards for serious vulnerabilities, leading to a 50% increase in the discovery of zero-click Remote Code Execution or cross-tenant vulnerabilities. Katie Moussouris, who played a key role in establishing the program, believes that while bug bounty programs are important, they should not replace secure software development. She advocates for a "concrete feedback loop," where bug bounty findings are integrated into secure development life cycles. Moussouris also suggests setting meaningful metrics to assess program success, such as reducing or eliminating classes of vulnerabilities. She also emphasizes the need for bug bounty programs to inform live incident response and threat intelligence. Despite the success of such programs, Moussouris does not believe they have made software more secure.



5 Years of Microsoft Bounty Programs

July 01, 2018 to June 30, 2023

<https://msrc.microsoft.com/blog/2023/11/celebrating-ten-years-of-the-microsoft-bug-bounty-program-and-more-than-60m-awarded/>

\$58.9M
in bounty rewards



22
Bounty programs



5,446
Eligible vulnerability
reports



1,117
Researchers awarded



\$200K
Biggest reward



Home > Conferences > CCS > Proceedings > CPSIoTSec '23 > The Internet of Insecure Cows - A Security Analysis of Wireless Smart Devices Used for Dairy Farming

SHORT-PAPER OPEN ACCESS



The Internet of Insecure Cows - A Security Analysis of Wireless Smart Devices Used for Dairy Farming

Authors: Samuel Barnes-Thornton, Joseph Gardiner, Awais Rashid [Authors Info & Claims](#)

CPSIoTSec '23: Proceedings of the 5th Workshop on CPS&IoT Security and Privacy • November 2023 • Pages 67–73

• <https://doi.org/10.1145/3605758.3623498>

<https://dl.acm.org/doi/10.1145/3605758.3623498>

Published: 26 November 2023 [Publication History](#)



0 citations 0 views



CPSIoTSec '23: Proceedings of the 5th...
The Internet of Insecure Cows - A...
Pages 67–73

← Previous Next →

ABSTRACT

References

ABSTRACT

IoT devices are becoming increasingly common in the world of agriculture with farmers now relying on technology to keep their businesses running. From crop management and greenhouse automation to entirely autonomous milking parlours, technology is being used in more ways than ever to improve efficiency. The benefits are huge, with the ability for farms to expand due to lower requirements for manual labour and other resources like water usage, so much so that in places it would now be infeasible for farmers to go back to traditional ways of working. Unfortunately, this technological



This research paper that examines the cybersecurity risks associated with the use of IoT devices in agriculture, specifically dairy farming & highlights how farmers are increasingly relying on technology for tasks such as crop management, greenhouse automation, and autonomous milking, which has led to increased efficiency and expansion opportunities. However, this technological advancement also increases the risk of cyber attacks, which could have devastating effects on individual farms and the wider food supply chain. The researchers conducted a detailed analysis of the security of collars used for health monitoring of cows in smart dairy farms. They successfully reverse-engineered the wireless protocol and demonstrated the ability to inject false data into the system, posing as one of the sensors. The tests revealed that both the system receiving signals from the sensors and the data endpoint software are vulnerable to data injection. The paper underscores the specific threats from these vulnerabilities and suggests potential countermeasures that could be integrated into the sensors in the future. The authors also reference instances of cyber attacks on farming cooperatives, emphasizing the real-world implications of their findings



ABSTRACT

References

efficiency. The benefits are huge, with the ability for farms to expand due to lower requirements for manual labour and other resources like water usage, so much so that in places it would now be infeasible for farmers to go back to traditional ways of working. Unfortunately, this technological



TOOL TIME





Sign In

[Join our Discord →](#)

havei**been**squatted?

Check if a domain has been typosquatted

example.com	Squatted?
-------------	-----------

<https://www.haveibeenstuffed.com/>

greynoise.io (10)

3209 permutations

Filter domains...

Columns ▾

Domain	Permutation	IPs	HTTP Banner	WHOIS/RDAP	
greynoise.org	TLD	198.185.159.144 198.185.159.145 198.49.23.144 198.49.23.145	Squarespace	<pre>{ "rdapConformance": ["rdap_level_0", "https://rdap.cloudflare.com"] }</pre> <p>Expand ↓</p>	
greynoise.in	TLD	216.239.34.21 216.239.32.21 216.239.36.21 216.239.38.21			
greynoise.ws	TLD	64.70.19.203			
greynoise.中国	TLD	218.241.105.10			
greynoise.com	TLD	64.187.239.229		<pre>{ "rdapConformance": ["rdap_level_0", "https://rdap.cloudflare.com"] }</pre> <p>Expand ↓</p>	
greynoise.中國	TLD	218.241.105.10			



Shameless Self-Promotion

<https://censys.com/tracking-vidar-infrastructure/>

BLOG

Tracking Vidar Infrastructure with Censys

SHARE    


NOVEMBER 21, 2023

Tags: [C2 Infrastructure](#), [Censys Search](#), [Research](#), [Threat Hunting](#)

Summary

Tracking Vidar Infrastructure

ABOUT THE AUTHOR



Aidan Holland
Security Researcher

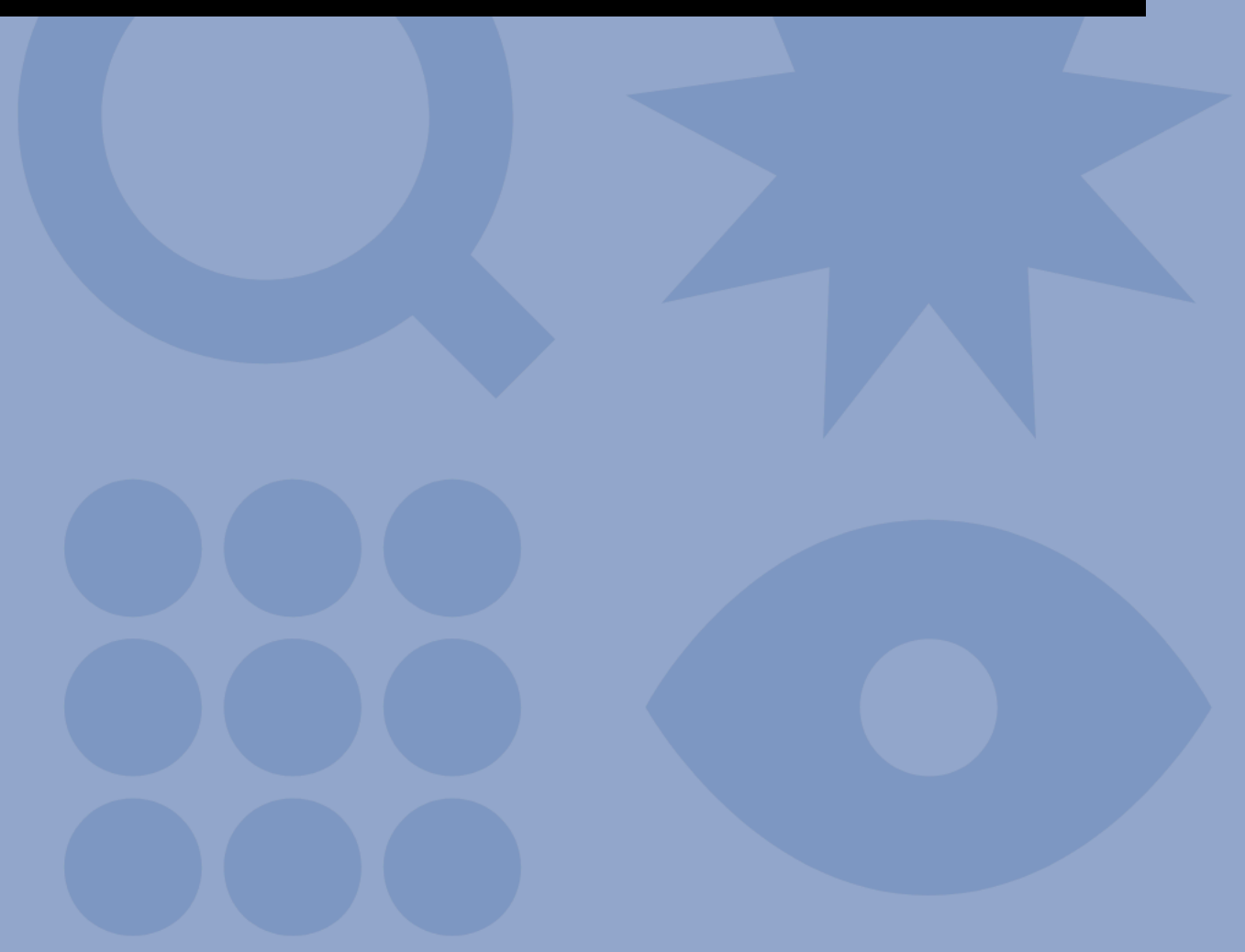
Aidan is a Security



```
https://censys.com/subtle-air-movements-and-femtosecond-response-times/
```

BLOG

Subtle Air Movements and Femtosecond Response Times



SHARE    

NOVEMBER 27, 2023

Tags: [External Attack Surface Management](#), [Internet Intelligence](#)

I'm a huge movie fan. Korean and French cinema are current favorites, but there's a special place in my heart for old martial arts flicks. You know the ones, utterly campy and unrealistic, but hugely entertaining. I'm thinking of those movies that showcase Jean Claude Van Damme

ABOUT THE AUTHOR



Nick Palmer
Sales Engineer / Customer Success Engineer

- 🏷️ Movable Type mt-upgrade.cgi RCE Attempt
- 🏷️ ownCloud Graph API Information Disclosure
- 🏷️ MantisBT SOAP API Version Check
- 🏷️ 74CMS SQL Injection Attempt

<https://viz.greynoise.io/trends?view=recent>

**WE NEED
TO TALK
ABOUT
KEY**



It Has Been

7

Days Since The
Last KEV Release

<https://observablehq.com/@greynoise/greynoise-tags>

❖ CVE-2023-4911: GNU C Library Buffer Overflow Vulnerability

<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



<https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>

[RESOURCES](#) [NEWSROOM](#) [ALERTS](#) [REPORT RANSOMWARE](#) [CISA.GOV](#)

[Home](#) / [Stop Ransomware](#)

I've Been Hit By Ransomware!

Ransomware Response Checklist



The Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends responding to ransomware by using the following checklist provided in a Joint CISA, FBI, NSA, and Multi-State Information Sharing and Analysis Center (MS-ISAC) [#StopRansomware Guide](#), updated in May 2023. This information will take you through the response process from detection to containment and eradication. Be sure to move through the first three steps in sequence.

Detection and Analysis

Refer to the best practices and references below to help manage the risk posed by ransomware and support your organization's coordinated and efficient response to a ransomware incident. Apply these practices to the greatest extent possible based on availability of organizational resources.

- **Determine which systems were impacted, and immediately isolate them.**

- If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems



CISA Known Exploited Vulnerabilities Catalog

<https://rud.is/kev/>

Last sync: 2023-11-27 18:13:04.

CISA recently made theirs both pretty and fairly useless, so here's a plain ol' table.

Go to [CISA's KEV Catalog page](#) to get CSV/JSON download links.

Show entries

Search:

cveID	vendorProject	product	vulnerabilityName	dateAdded	shortDescription	requiredAction	dueDa
CVE-2023-4911	GNU	GNU C Library	GNU C Library Buffer Overflow Vulnerability	2023-11-21	GNU C Library's dynamic loader ld.so contains a buffer overflow vulnerability when processing the GLIBC_TUNABLES environment variable, allowing a local attacker to execute code with elevated privileges.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-12
CVE-2023-36584	Microsoft	Windows	Microsoft Windows Mark of the Web (MOTW) Security Feature Bypass Vulnerability	2023-11-16	Microsoft Windows Mark of the Web (MOTW) contains a security feature bypass vulnerability resulting in a limited loss of integrity and availability of security features.	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.	2023-107
CVE-			Sophos Web		Sophos Web Appliance contains a command	Apply mitigations per vendor instructions or	





Storm ⚡ Watch